

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

NATALIE DELGADO,

Plaintiff,

v.

META PLATFORMS, INC.,

Defendant.

Case No. [23-cv-04181-SI](#)

**ORDER GRANTING IN PART AND
DENYING IN PART MOTION TO
DISMISS**

Re: Dkt. No. 35

Defendant Meta Platforms, Inc. (“Meta”) moves to dismiss the putative class action complaint in this case. The matter came on for hearing on February 23, 2024. For the reasons set forth below, the Court GRANTS IN PART and DENIES IN PART the motion to dismiss.

BACKGROUND

“Illinois’s Biometric Information Privacy Act, familiarly known as BIPA, provides robust protections for the biometric information of Illinois residents. See 740 ILCS 14/1 *et seq.* It does so by regulating the collection, retention, disclosure, and destruction of biometric identifiers or information—for example, retinal scans, fingerprints, or facial geometry.” *Thornley v. Clearview AI, Inc.*, 984 F.3d 1241, 1242 (7th Cir. 2021). At issue in this case is the collection of “voiceprints.”

Plaintiff Natalie Delgado is an Illinois citizen who alleges that defendant Meta took her voiceprint without complying with the requirements of BIPA. Meta owns and operates the social media platform Facebook as well as the messaging application Messenger. Dkt. No. 1 (“Compl.”) ¶¶ 2-3. Plaintiff sues on behalf of herself and a putative class consisting of: “All natural persons in Illinois from whom Meta created, collected, captured, received, obtained, or stored Digital Voice Data, Voice Characteristics, and/or a Voice Profile.” *Id.* ¶ 153. Plaintiff, on behalf of the proposed

class, seeks statutory damages under BIPA, an injunction, and attorneys' fees and costs.

LEGAL STANDARD

Under Federal Rule of Civil Procedure 12(b)(6), a district court must dismiss a complaint if it fails to state a claim upon which relief can be granted. To survive a Rule 12(b)(6) motion to dismiss, the plaintiff must allege "enough facts to state a claim to relief that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). This "facial plausibility" standard requires the plaintiff to allege facts that add up to "more than a sheer possibility that a defendant has acted unlawfully." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). Although courts do not require "heightened fact pleading of specifics," *Twombly*, 550 U.S. at 544, a plaintiff must provide "more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do." *Id.* at 555. The plaintiff must allege facts sufficient to "raise a right to relief above the speculative level." *Id.*

In deciding whether the plaintiff has stated a claim, the Court must assume that the plaintiff's allegations are true and must draw all reasonable inferences in his or her favor. *Usher v. City of Los Angeles*, 828 F.2d 556, 561 (9th Cir. 1987). However, the Court is not required to accept as true "allegations that are merely conclusory, unwarranted deductions of fact, or unreasonable inferences." *St. Clare v. Gilead Scis., Inc.*, 536 F.3d 1049, 1055 (9th Cir. 2008). As a general rule, the Court may not consider any materials beyond the pleadings when ruling on a Rule 12(b)(6) motion. *Lee v. City of Los Angeles*, 250 F.3d 668, 688 (9th Cir. 2001). However, pursuant to Federal Rule of Evidence 201, the Court may take judicial notice of "matters of public record," such as prior court proceedings. *Id.* at 688-89. The court may also consider "documents attached to the complaint [and] documents incorporated by reference in the complaint . . . without converting the motion to dismiss into a motion for summary judgment." *United States v. Ritchie*, 342 F.3d 903, 908 (9th Cir. 2003).

If the Court dismisses the complaint, it must then decide whether to grant leave to amend. The Ninth Circuit has "repeatedly held that a district court should grant leave to amend even if no request to amend the pleading was made, unless it determines that the pleading could not possibly

be cured by the allegation of other facts.” *Lopez v. Smith*, 203 F.3d 1122, 1130 (9th Cir. 2000) (citations and internal quotation marks omitted).

DISCUSSION

Defendant moves to dismiss the complaint on several grounds. First, defendant argues that California law, and not Illinois law, governs because the Terms of Service that plaintiff agreed to when she used Facebook and Messenger contain a California choice-of-law clause. Second, defendant argues that even if Illinois law were to apply, plaintiff has not plausibly alleged that Meta collected her “voiceprint” as opposed to merely her “voice recording.” Third, defendant argues the complaint fails to plausibly allege claims under BIPA Sections 15(c) and 15(e), regarding whether Meta “profited” from plaintiff’s biometric data or failed to store the data with the care required by statute.¹

I. Choice-of-Law

Federal courts sitting in diversity ordinarily apply the choice-of-law rules of the forum state – here, California. *See Atl. Marine Const. Co. v. U.S. Dist. Court for W. Dist. of Tex.*, 571 U.S. 49, 65 (2013). The parties agree that California choice-of-law rules govern.

In California, where the parties’ contract contains a choice-of-law provision, courts “apply the principles set forth in Restatement section 187, which reflects a strong policy favoring enforcement of such provisions.” *Nedlloyd Lines B.V. v. Superior Court*, 3 Cal. 4th 459, 464-65 (1992). Under this approach, the court first determines as a threshold matter “(1) whether the chosen state has a substantial relationship to the parties or their transaction, or (2) whether there is any other reasonable basis for the parties’ choice of law.” *Id.* at 466. “If . . . either test is met, the court must next determine whether the chosen state’s law is contrary to a *fundamental* policy of” the alternative state’s law. *Id.*; *see also In re Facebook Biometric Info. Priv. Litig.*, 185 F. Supp. 3d 1155, 1169 (N.D. Cal. 2016). If there is a fundamental conflict, “the court must then determine whether [the

¹ In this Order, the Court uses the term “biometric data” to encompass both “biometric identifiers” and “biometric information” as defined in BIPA. *See* 740 ILCS 14/10.

alternative state] has a ‘materially greater interest than the chosen state in the determination of the particular issue’” *Nedlloyd Lines*, 3 Cal. 4th at 466 (quoting Rest., § 187, subd. (2)); *see also Wash. Mut. Bank, FA v. Superior Court*, 24 Cal. 4th 906, 916 (2001). “In determining which state has a materially greater interest, California courts ‘consider which state, in the circumstances presented, will suffer greater impairment of its policies if the other state’s law is applied.’” *Ruiz v. Affinity Logistics Corp.*, 667 F.3d 1318, 1324-25 (9th Cir. 2012) (quoting *Brack v. Omni Loan Co., Ltd.*, 164 Cal. App. 4th 1312, 1329 (2008)).

Plaintiff, as the party opposing enforcement of the choice-of-law provision, “bears the burden to establish a fundamental conflict in the states’ laws and the nondesignated state’s materially greater interest in the determination of the particular issue.” *See Colaco v. Cavotec SA*, 25 Cal. App. 5th 1172, 1188-89 (2018) (citing *Wash. Mut. Bank*, 24 Cal. 4th at 917). Here, plaintiff does not seriously dispute that California has a substantial relationship to the parties or their transaction. The question, then, is whether California’s law is contrary to a fundamental policy of Illinois law and, if so, whether Illinois has a materially greater interest than California in the determination of the particular issue.

The district court weighed those precise questions with respect to BIPA and a Facebook user agreement in *In re Facebook Biometric Information Privacy Litigation* and determined that “[t]he answer to both questions is yes.” 185 F. Supp. 3d at 1169. The Court finds the analysis of *Facebook Biometric* regarding choice-of-law well reasoned and applicable to the facts at hand and repeats the relevant portion of the decision here:

There can be no reasonable doubt that the Illinois Biometric Information Privacy Act embodies a fundamental policy of the state of Illinois. “To be fundamental within the meaning of Restatement section 187, a policy must be a substantial one.” *Brack v. Omni Loan Co.*, 164 Cal. App. 4th 1312, 1323, 80 Cal. Rptr. 3d 275 (2008). By its express terms, BIPA manifests Illinois’ substantial policy of protecting its citizens’ right to privacy in their personal biometric data. . . .

It is equally undeniable that enforcing the contractual choice of California law would be contrary to this policy in the starkest way possible. Facebook tries to downplay the conflict as merely the loss of a claim. . . . But if California law is applied, the Illinois policy of protecting its citizens’ privacy interests in their biometric data,

1 especially in the context of dealing with “major national corporations” like
2 Facebook, would be written out of existence. That is the essence of a choice-of-law
3 conflict. . . . The conflict is all the more pronounced because California has no law
4 or policy equivalent to BIPA. Unlike Illinois, California has not legislatively
5 recognized a right to privacy in personal biometric data and has not implemented any
6 specific protections for that right or afforded a private cause of action to enforce
7 violations of it. . . .

8 Illinois’ greater interest in the outcome of this BIPA dispute is also readily apparent.
9 The fundamental question on this point is “which state, in the circumstances
10 presented, will suffer greater impairment of its policies if the other state’s law is
11 applied.” *Bridge Fund Capital Corp. v. Fastbucks Franchise Corp.*, 622 F.3d 996,
12 1004 (9th Cir.2010) (citing *Brack*, 164 Cal.App.4th at 1329, 80 Cal.Rptr.3d 275).
13 The answer here could not be clearer. Illinois will suffer a complete negation of its
14 biometric privacy protections for its citizens if California law is applied. In contrast,
15 California law and policy will suffer little, if anything at all, if BIPA is applied.

16 *Id.* at 1169-70 (citations omitted). Numerous courts have since cited *Facebook Biometric* when
17 applying Illinois law rather than the state law provided for in various technology companies’ user
18 agreements. *See, e.g., Patterson v. Respondus, Inc.*, 593 F. Supp. 3d 783, 811-13 (N.D. Ill. 2022);
19 *Hogan v. Amazon.com, Inc.*, No. 21 C 3169, 2022 WL 952763, at *4-5 (N.D. Ill. Mar. 30, 2022);
20 *see also Vance v. Microsoft Corp.* (“*Vance I*”), 534 F. Supp. 3d 1301, 1312 (W.D. Wash. 2021)
21 (citing *Facebook Biometric* for the proposition that applying Washington law to unjust enrichment
22 claims would cause Illinois to suffer the greater impairment of its policies, in light of BIPA).

23 There is a notable distinction in this case, which defendant raises in its motion. *See* Dkt. No.
24 35 (“Mot.”) at 11. *Facebook Biometric* was decided in 2016, before passage of the California
25 Consumer Privacy Act of 2018 and its subsequent amendment by the California Privacy Rights Act
26 of 2020 (collectively, “CCPA”). “The purpose of the CCPA . . . was to protect consumers’ privacy
27 rights by providing them meaningful control over how their personal information is collected, used,
28 and disclosed by a covered business.” *Cal. Privacy Prot. Agency v. Superior Ct. of Sacramento*
Cnty., No. C099130, --- Cal. Rptr. 3d ---, 2024 WL 509994, at *1 (Cal. Ct. App. Feb. 9, 2024).
Defendant argues that BIPA does not fundamentally conflict with California’s more recently
enacted privacy laws and that, even if there were a fundamental conflict, Illinois does not have a

1 materially greater interest in the outcome of this case.

2 Plaintiff points to numerous ways in which BIPA and the CCPA differ, with BIPA providing
3 protections and rights that the CCPA does not. Dkt. No. 47 (“Opp’n”) at 7-9. For several reasons,
4 the Court is persuaded that applying California law would run contrary to fundamental Illinois
5 policy. First, the CCPA does not apply to Illinois citizens. *See* Cal. Civ. Code § 1798.140(i)
6 (defining “Consumer” as “a natural person who is a California resident . . .”).² In attempting to
7 distinguish *Facebook Biometric*, defendant glosses over this critical fact. As defendant
8 acknowledges, the *Facebook Biometric* court found that there was a fundamental policy conflict
9 between California and Illinois law in part because applying California law would “writ[e] out of
10 existence” the “Illinois policy of protecting **its citizens’** privacy interests in their biometric data.”
11 Mot. at 11 (quoting *Facebook Biometric*, 185 F. Supp. 3d at 1169) (emphasis added). Defendant
12 notes in the reply brief that the CCPA applies to persons who are residing in California more than
13 temporarily and speculates that perhaps plaintiff is one such person. *See* Dkt. No. 52 (“Reply”) at
14 2 n.1. But defendant does not otherwise seriously contend that the CCPA applies to Illinois
15 residents.

16 Second, BIPA provides a private right of action, allowing for statutory damages and
17 reasonable attorneys’ fees and costs, by “[a]ny person aggrieved by a violation of this Act[.]” 740
18 ILCS 14/20. The CCPA, by contrast, calls for enforcement by the California Attorney General,
19 allowing a private right of action only in the event of a security breach. *See* Cal. Civ. Code
20 § 1798.150 (Personal Information Security Breaches). Defendant attempts to minimize this

21
22 ² In full, the relevant definition of “consumer” in the CCPA reads: “(i) “Consumer” means
23 a natural person who is a California resident, as defined in Section 17014 of Title 18 of the California
24 Code of Regulations, as that section read on September 1, 2017, however identified, including by
25 any unique identifier.” Cal. Civ. Code § 1798.140(i).

26 On September 1, 2017, California Code of Regulations Section 17014 of Title 18, read, in
27 relevant part:

28 The term “resident,” as defined in the law, includes (1) every individual who is in
the State for other than a temporary or transitory purpose, and (2) every individual
who is domiciled in the State who is outside the State for a temporary or transitory
purpose. All other individuals are nonresidents.

Cal. Code Regs. tit. 18, § 17014.

1 difference. According to defendant, the private right of action contained in “[t]he CCPA reflects
2 California’s public policy of allowing consumers to seek redress for *actual harm* for statutory
3 violations, while reserving to the State the power to seek penalties for technical violations that
4 caused no harm.” Mot. at 10 n.4 (emphasis added).

5 This highlights one of the fundamental conflicts between California and Illinois law: BIPA’s
6 private right of action reflects “the legislature’s judgment that a violation of BIPA’s *procedures*
7 would cause actual and concrete harm. . . . When an online service simply disregards the Illinois
8 procedures, as Facebook is alleged to have done, the right of the individual to maintain her biometric
9 privacy vanishes into thin air. The precise harm the Illinois legislature sought to prevent is then
10 realized.” *Patel v. Facebook Inc.*, 290 F. Supp. 3d 948, 953-54 (N.D. Cal. 2018) (emphasis added)
11 (analyzing BIPA in the standing context); *see also* ILCS 14/5(c) (Illinois General Assembly finding,
12 *inter alia*, “Biometrics are unlike other unique identifiers that are used to access finances or other
13 sensitive information. For example, social security numbers, when compromised, can be changed.
14 Biometrics, however, are biologically unique to the individual; therefore, once compromised, the
15 individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from
16 biometric-facilitated transactions.”). A number of district courts have found it determinative in
17 BIPA choice-of-law cases whether the alternative state provides a private right of action. *See*
18 *Patterson*, 593 F. Supp. 3d at 811-12; *Hogan*, 2022 WL 952763, at *4.

19 Tellingly, none of the cases on which defendant relies involved BIPA. Defendant instead
20 relies on various cases analyzing consumer protection laws. But those cases provide little guidance
21 to this Court regarding BIPA’s application. As one district court observed, in ruling against Amazon
22 on a similar issue: “The line of cases that Amazon cites is evidence that courts do not consider the
23 Consumer Fraud Act to be fundamental Illinois public policy, but it sheds no light on the status of
24 BIPA. Every state has a consumer protection law, most of which allows individuals to file suit on
25 their own behalf. [Citation.] That is not the case at hand. Thus, the Court finds that the
26 [Washington] choice-of-law provision is contrary to Illinois’ fundamental public policy in this
27 case.” *Hogan*, 2022 WL 952763, at *4.

28 In sum, the Court agrees with plaintiff that the enactment of the CCPA does not change the

analysis contained in *Facebook Biometric*. For the reasons stated in that decision, *see* 185 F. Supp. 3d at 1169-70, the Court finds that: California law conflicts with a fundamental policy of Illinois law, as embodied in BIPA; and Illinois has a materially greater interest in the outcome of this BIPA dispute. The Court will apply Illinois law to plaintiff's claims.

II. Voiceprint Allegations

Defendant additionally argues that, as a pleading matter, the complaint fails plausibly to allege that Meta collects voiceprints (either plaintiff's or anyone else's) in violation of BIPA. BIPA regulates how private entities may retain, collect, disclose, and destroy "biometric identifiers" and "biometric information." *See generally* 740 ILCS 14/15. "'Biometric identifier' means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." 740 ILCS 14/10. The statute also includes a long list of what "biometric identifiers" do not include: writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, and more. *See id.* "'Biometric information' means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual. Biometric information does not include information derived from items or procedures excluded under the definition of biometric identifiers." *Id.* The statute does not define the term "voiceprint."

Plaintiff's claims here depend upon BIPA's regulation of "voiceprints." Defendant argues that she has alleged nothing more than Meta's recording of her voice and, according to defendant, a "voiceprint" under BIPA is something more than a "voice recording." Mot. at 14. Defendant argues that the only support plaintiff provides for her allegations are: (1) a patent and its continuations that Meta owns, and (2) a statement in Meta's United States Regional Privacy Notice regarding the collection of voice recordings. As to the patent, defendant argues that ownership of a patent shows only that Meta has the right to exclude others from practicing the claimed invention and that it does not show Meta actually practices the technology. Mot. at 15-17. As to the privacy notice, defendant argues this relates to its disclosure obligations under the CCPA, which regulates voice recordings but not voiceprints. *Id.* at 17. Defendant further argues that neither the patent nor the privacy notice

are specific to Facebook or Messenger and so plaintiff has not shown that defendant collected *her* voiceprints when she used those particular services. *Id.* at 17-18.

At this stage, the Court treats as true the factual allegations as stated in plaintiff’s complaint and draws all reasonable inferences in her favor. *See Usher*, 828 F.2d at 561. Viewing the allegations as a whole, the Court finds plaintiff has sufficiently alleged that Meta has collected her voiceprint. Meta’s arguments, many of which essentially seek to impose a heightened pleading standard, are more appropriately considered at a later stage of the case. That plaintiff pleads some of the facts “on information and belief” does not change that analysis. *See Cothron v. White Castle Sys., Inc.*, 467 F. Supp. 3d 604, 618 (N.D. Ill. 2020) (“[t]he *Twombly* plausibility standard . . . does not prevent a plaintiff from pleading facts alleged upon information and belief where the facts are peculiarly within the possession and control of the defendant.”) (quoting *Arista Records, LLC v. Doe 3*, 604 F.3d 110, 120 (2d Cir. 2010)).

Plaintiff is a citizen of Illinois who has a Facebook account and utilizes Meta’s Messenger application. Compl. ¶¶ 25, 148. On multiple occasions in 2023, 2022, and “throughout the Class Period, Plaintiff has, for personal use, input her voice into an audio function on Facebook or Messenger, including, *inter alia*, to dictate text messages to send via Messenger, sending an audio recording of her voice via Messenger, and making audio calls via Messenger.”³ *Id.* ¶ 149.

The complaint alleges that in December 2016, Meta (at that time Facebook, Inc.) filed a patent application seeking “to protect methods, software, and processors for identifying users of its social networks with voiceprints created from audio input into the social network site or related applications[.]” *Id.* ¶¶ 52-53. The methods protected by the patent describe voiceprint technology, in that they describe methods for recording and analyzing a user’s voice “to determine a digital voiceprint for the user[.]” which the social-networking system may then use to identify or authenticate the user based on audio input. *See id.* ¶ 56. The patent was issued March 31, 2020 (“the 2020 Voiceprint Patent”) and Meta has since filed several patent applications that incorporated and were continuations of the patent. *Id.* ¶¶ 67, 70, 73.

³ The complaint defines the “Class Period” as “that period within the statute of limitations for this action and extending until a Class is certified herein.” Compl. ¶ 157.

1 The complaint further describes the method by which plaintiff alleges Meta captures, creates,
2 collects, and stores voiceprints. *Id.* ¶¶ 82-97. Among other things, plaintiff alleges Meta uses the
3 audio input into Facebook or Messenger or otherwise received by Meta to create encoded digital
4 data of the acoustic signals of the speaker’s voice, and that data is then processed with an acoustical
5 model that is then trained and further refined using the voice of a particular speaker such that the
6 acoustical model can be used to recognize that user by voice. *Id.* ¶¶ 83-85. The complaint also
7 alleges, “The acoustical model is further trained using the voices of many users to produce a speaker-
8 independent model capable of recognizing multiple users by their voice.” *Id.* ¶ 86.

9 The complaint alleges that, for the first time beginning in January 2023, Meta added terms
10 to its “United States Regional Privacy Notice” that revealed to Meta users “that it can use audio of
11 voices to identify users.” *Id.* ¶¶ 131, 140. Specifically, the notice states that Meta may collect
12 “‘sensitive personal information’ (as defined in the privacy laws of California, Colorado,
13 Connecticut, Utah, and Virginia)” including “voice recordings which may be used to identify you
14 when you use relevant features.” *Id.* ¶ 139.

15 Taking these allegations together, the Court finds that plaintiff has sufficiently alleged that
16 Meta has collected her voiceprint as regulated by BIPA. Meta argues that plaintiff has not alleged
17 her “voiceprint” was captured because she has not alleged that Meta *actually* identified her using
18 the voice recordings that it collected. The Court agrees with the line of cases analyzing BIPA in
19 which district courts, “utilizing statutory text and dictionary definitions of the term, have defined
20 [“voiceprint”] as data unique to an individual that *could be used* to identify someone” rather than as
21 data that *was used* to identify someone. *See Robinson v. Lake Ventures LLC*, No. 22 CV 6451, 2023
22 WL 5720873, at *7 (N.D. Ill. Sept. 5, 2023) (citing *Vance v. Int’l Bus. Machines Corp.*, No. 20 C
23 577, 2020 WL 5530134, at *5 (N.D. Ill. Sept. 15, 2020)); *see also Carpenter v. McDonald’s Corp.*,
24 580 F. Supp. 3d 512, 518 (N.D. Ill. 2022) (“pursuant to the plain language of the statute, a defendant
25 may violate BIPA by collecting a voiceprint that merely *could be used* to identify a plaintiff”);
26 *Daichendt v. CVS Pharmacy, Inc.*, No. 22 CV 3318, 2022 WL 17404488, at *5 (N.D. Ill. Dec. 2,
27 2022) (“The court disagrees with defendant that plaintiffs must specifically allege that defendant, in
28 fact, “used” their biometric data to determine their identities. Instead, plaintiffs must allege that

defendant’s collection of their biometric data made defendant capable of determining their identities”), *modified on reconsideration*, No. 22 CV 3318, 2023 WL 3579082 (N.D. Ill. Feb. 3, 2023) (citation omitted). The defendants in those cases all made the same argument that Meta makes here, that the plaintiff must show the defendant actually used the data to identify plaintiff in order to implicate BIPA, and the courts rejected that contention at the motion to dismiss stage. Plaintiff here has not alleged that Meta in fact used her voice data to identify her, but under the case law coming out of the Northern District of Illinois, she need not have done so.

The Court further finds it is proper to consider plaintiff’s allegations regarding the privacy notice and the patents in ruling on the motion to dismiss.⁴ Defendant argues that the U.S. Regional Privacy Notice cited in the complaint is targeted towards compliance with the CCPA (which it says regulates “voice recordings”) and does not concede Meta’s collection of voiceprints in violation of BIPA. Mot. at 17; Reply at 10-11. But on its face, the privacy notice states that it “is for people living in the United States[,]” not simply in California. *See* Dkt. No. 35-4, Chorba Decl., Ex. B at 1. The notice goes on to state: “This Notice explains how we collect, use, and disclose your Personal Information. It **also** describes how to exercise your rights under the California Consumer Privacy Act” *Id.* (emphasis added). Thus, the notice by its own terms is not limited to the CCPA or to California residents. That the notice uses the definition of “Personal Information” as contained in the CCPA does not change this. *See id.* at 2. The notice states that Meta may collect “voice recordings which may be used to identify you when you use relevant features.” *Id.* at 4. Voice recordings *which may be used to identify a person* are more than mere “voice recordings.” At this stage, plaintiff’s allegations are sufficient. Meta may challenge the applicability of the U.S. Regional Privacy Notice upon a fuller factual record.

As to the patents, in *Carpenter v. McDonald’s Corporation*, the district court found

⁴ Meta attaches the privacy policy, privacy notice, and terms of service that plaintiff references in her complaint. Dkt. No. 35-2 (“Chorba Decl.”). Plaintiff does not oppose the Court considering these documents for the limited purposes stated in the motion. Opp’n at 6 n.1. The Court finds these documents are properly incorporated by reference and/or are subject to judicial notice and therefore considers them on this motion to dismiss, without converting the motion into one for summary judgment. *See Khoja v. Orexigen Therapeutics, Inc.*, 899 F.3d 988, 1002 (9th Cir. 2018).

allegations relying on the defendant’s voice assistant technology patent were sufficient to survive a motion to dismiss.⁵ 580 F. Supp. 3d at 517. As in *Carpenter*, “[b]ased on the facts pleaded in the complaint, including the referenced Patent, it is reasonable to infer—though far from proven—that Defendant’s technology mechanically analyzes customers’ voices in a measurable way such that [Meta] has collected a voiceprint from Plaintiff and other [users].” *See id.* Whether or not Meta actually practices the technology described in the voiceprint patents may be appropriately litigated down the line.⁶

In sum, the Court need not resolve the question Meta raises of whether a “voiceprint” under BIPA means something more than a “voice recording” because plaintiff alleges more than simply the collection of her voice recording.

Finally, the Court declines Meta’s request to dismiss the allegations as to third-party voiceprint collection. The very nature of those allegations is that Meta is collecting plaintiff’s voiceprint without her knowledge or consent, “via other users utilizing Facebook or Messenger and/or via third parties.” Compl. ¶ 150. In quoting from Meta’s 2020 Voiceprint Patent, the complaint cites to several examples of how this may occur. For instance, a “media device” belonging to Marsha and “associated with the social-networking system” may: receive the voice of Jan when Jan is at Marsha’s house watching TV; identify Jan based on her voiceprint and her social-graph connection to Marsha; and then feed content and advertisements to Marsha and Jan accordingly. *Id.* ¶ 61. The patent also provides a scenario where a third party (such as a Bluetooth beacon in a store) may detect a customer speaking and identify them, based on their voiceprint and their social-networking connection to another person who is known to be in the store. *Id.* ¶ 62. Whether or not Meta is actually doing this and whether or not the “social-networking system” referred to in the patent includes Facebook or Messenger are all factual questions to resolve at a

⁵ The *Carpenter* court allowed the Section 15(b) claims under BIPA to proceed, while dismissing claims brought under Section 15(d). Section 15(d) is not at issue here.

⁶ To the extent that Meta argues that the patents are not tied to plaintiff’s claims because the patents “make no mention of Facebook or Messenger,” the Court notes that the complaint alleges it was Facebook, Inc. that applied for the original patent in 2016, before Meta existed. *See* Compl. ¶ 52.

later stage. The Court finds the third-party collection allegations sufficient at this time.

III. Section 15(c) Claim

Defendant independently moves to dismiss Count III, brought under Section 15(c) of BIPA. Section 15(c) states: “No private entity in possession of a biometric identifier or biometric information may sell, lease, trade, or otherwise profit from a person’s or a customer’s biometric identifier or biometric information.” 740 ILCS 14/15(c).

Section 15(c) “regulates transactions with two components: (1) access to biometric data is shared or given to another; and (2) in return for that access, the entity receives something of value.” *Vance v. Amazon.com Inc.* (“*Vance I*”), 534 F. Supp. 3d 1314, 1322 (W.D. Wash. 2021). District courts are generally in agreement that Section 15(c) of BIPA “does not require a direct sale of biometric data.” *See Mayhall on behalf of D.M. v. Amazon Web Servs. Inc.*, No. C21-1473-TL-MLP, 2022 WL 2718091, at *12 (W.D. Wash. May 24, 2022), *report and recommendation adopted*, 2023 WL 2728292 (W.D. Wash. Mar. 31, 2023) (citations omitted). The first component may be met where, for instance, “the biometric data may be so integrated into a product that consumers necessarily gain access to biometric data by using the product or service.” *Vance II*, 534 F. Supp. 3d at 1322. As to the second component, the use of the term “otherwise profit” in Section 15(c) need not “be limited to a pecuniary benefit. Section 15(c) prohibits the commercial dissemination of biometric data for some sort of gain, whether pecuniary or not.” *Id.* In other words, “[b]y prohibiting for-profit transactions involving biometric data, [Section 15(c)] aims to control the spread of biometric data.” *Id.* at 1323 n.4 (citing *Thornley*, 984 F.3d at 1247).

Here, plaintiff’s theory rests on the allegation that Meta uses “technology that is so intertwined with the biometric data that marketing the Meta voice-recognition technology and targeted content that utilizes it is essentially disseminating biometric data for profit.” *See* Compl. ¶ 188; *see also id.* ¶ 186 (alleging that Meta used the biometric data to improve its natural language understanding and machine learning, expand the scope of Meta’s products, provide targeted content

1 and advertising, and create other business opportunities).⁷

2 In her opposition brief, plaintiff points to various statements in the U.S. Regional Privacy
3 Notice, arguing that because Meta says it may disclose “Personal Information” (which plaintiff
4 states includes voiceprints) to “[a]pps, websites, and third-party integrations” or to “[p]artners,
5 including partners offering goods and services on our products” Meta has therefore admitted to
6 commercial dissemination of biometric data. Opp’n at 24 (citing Compl. ¶ 141). The Court agrees
7 with defendant that these allegations are too attenuated to make a violation of Section 15(c)
8 plausible.

9 As defendant notes, all of the cases on which plaintiff relies involved defendants that
10 provided a third party with access to data, or to a product that heavily incorporated biometric data,
11 in exchange for consideration. *See* Reply at 14. For instance, in *Vance II*, photos that the plaintiffs
12 had uploaded to a photo sharing site became part of a dataset that Amazon ultimately used to create
13 a facial recognition product called “Rekognition,” which Amazon marketed to customers such as
14 the FBI. The complaint alleged that Rekognition’s face-matching feature was incorporated into
15 many Amazon products and that Amazon’s customers used Rekognition to monitor people of
16 interest. *Vance II*, 534 F. Supp. 3d at 1324. The court found the allegations “support the inference
17 that the biometric data is itself so incorporated into Amazon’s product that by marketing the product,
18 it is commercially disseminating the biometric data.” *Id.* (citation omitted). In another example
19 cited, the defendants created and sold access to a database of biometric information generated from
20 photographs of plaintiffs collected by scraping public websites. *In re Clearview AI, Inc., Consumer*
21 *Privacy Litig.*, 585 F. Supp. 3d 1111 (N.D. Ill. Feb. 14, 2022). In finding the Section 15(c)
22 allegations sufficient to survive a motion to dismiss, the court explained, “At its core, plaintiffs’
23 claim concerns the sale of biometric data because the Clearview defendants’ business model is
24 premised on collecting and capturing biometric data and then profiting from that data when
25 customers pay to search the Clearview database.” *Id.* at 1126; *see also Mahmood v. Berbix, Inc.*,

26
27 ⁷ Plaintiff also asserts that Meta violates Section 15(c) “by selling, leasing, trading, or
28 otherwise profiting from Plaintiff’s and Class Members’ biometric identifiers and/or biometric
information in its possession,” but the Court finds the allegations as to selling, leasing, or trading
are conclusory. *See* Compl. ¶ 190.

No. 22 C 2456, 2022 WL 3684636 (N.D. Ill. Aug. 25, 2022) (complaint alleged that a rental car service paid for access to the defendant’s facial recognition platform to verify plaintiff’s age and identity before she rented the car); *Mayhall*, 2022 WL 2718091, at *12 (complaint “clearly pleaded that access to D.M.’s biometric data was shared or disseminated to Take-Two, and that in return for that access, Defendants received something of value—namely payment from Take-Two”).

Here, plaintiff has not pleaded any facts similar to those found in the cases she cites. She does not allege that Meta has created a “product” from her biometric data or that Meta marketed a product containing her biometric data or that Meta so incorporated her voiceprint into its technology that selling its products necessarily meant selling access to her data. It is not clear from the complaint what “product” plaintiff is alleging Meta markets. At least one district court has held that it is insufficient to allege, without more, that a company used biometric data to improve its technologies, which improved the effectiveness of its products and made them more commercially valuable. *See Vance I*, 534 F. Supp. 3d at 1309. That is essentially what plaintiff is alleging here.

Accordingly, the Court GRANTS the motion to dismiss the Section 15(c) claim, with leave to amend. As discussed at the hearing, the parties did not brief the issue of Article III standing. In amending, plaintiff may also add allegations to demonstrate that she has standing to bring this claim. *See Thornley*, 984 F.3d at 1246-47.

IV. Section 15(e) Claim

Lastly, defendant moves to dismiss Count IV, brought for violations of Section 15(e) of BIPA. That section states:

(e) A private entity in possession of a biometric identifier or biometric information shall:

(1) store, transmit, and protect from disclosure all biometric identifiers and biometric information using the reasonable standard of care within the private entity’s industry; and

(2) store, transmit, and protect from disclosure all biometric identifiers and biometric information in a manner that is the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information.

1 740 ILCS 14/15(e). Courts have explained that “section 15(e) requires that private entities protect
2 biometric information from disclosure.” *See Namuwonge v. Kronos, Inc.*, 418 F. Supp. 3d 279, 285
3 (N.D. Ill. 2019) (citations omitted).
4

5 Here, the Court agrees with defendant that the allegations of the complaint are conclusory
6 and fail to put defendant on notice of the challenged conduct. The complaint recites the elements
7 of Section 15(e), but the only underlying factual allegations plaintiff cites in support are: that “Meta
8 acknowledges that its large size and vast amount of user data makes [sic] it a key target for cyber-
9 attacks, has disclosed it has been the subject of cyber-attacks in the past, states it will be subject to
10 future intrusions, and admits it may not be aware of or discover all such intrusions.” *See Compl.*
11 ¶ 198. The complaint provides no allegations regarding how Meta stores biometric data or how its
12 practices fail to comply with the reasonable standard of care. Without more, the fact that a company
13 has been and may again be subject to cyber-attacks does not make it plausible that the company has
14 violated an industry-wide standard of care for purposes of Section 15(e) of BIPA.

15 The Court GRANTS the motion to dismiss the Section 15(e) claim, with leave to amend.


16 CONCLUSION

17 For the foregoing reasons and for good cause shown, the Court hereby GRANTS IN PART
18 and DENIES IN PART the motion to dismiss. The Section 15(c) and 15(e) claims are dismissed,
19 with leave to amend. The balance of the motion is denied.
20

21 **Any amended complaint shall be filed no later than March 15, 2024.**

22 **IT IS SO ORDERED.**

23 Dated: February 27, 2024

24 
25 _____
26 SUSAN ILLSTON
27 United States District Judge
28